Weak Systems Have Intractable Theorems

Raheleh Jalali

LATD 2022 and MOSAIC Kick off Meeting

6 September, 2022

The aim

Problem

Studying the "strengths" of proof systems.

By strength we mean:

- Proof theory: *provability* of a theorem. (Potential proofs)
- Proof complexity: *feasibility* of the proofs. (Actual proofs)

The latter leads to the quantitative study of the proofs: determining the minimal "complexity" of a proof of a theorem in a given "proof system".

Formalizing the concept of proof

There are many different formalizations of the concept of a proof. The basic property: being a proof must be easy to check (polynomial time).

Definition [Cook, Reckhow '79]

Propositional proof system: a poly-time function **P** whose range is the set of all propositional tautologies. If $\mathbf{P}(x) = \varphi$, we call x a **P**-proof of φ.

(Proofs and formulas are encoded as strings in a finite alphabet.)

Examples: The usual Hilbert-style and Gentzan-style proof systems.

Connection to complexity theory

An immediate but fundamental observation:

Theorem

(Cook, Reckhow '79) There exists a polynomially bounded proof system, i.e., a proof system for propositional logic in which all tautologies have proofs of polynomial length, if and only if NP = coNP.

Connection to complexity theory

An immediate but fundamental observation:

Theorem

(Cook, Reckhow '79) There exists a polynomially bounded proof system, i.e., a proof system for propositional logic in which all tautologies have proofs of polynomial length, if and only if NP = coNP.

Proof.

Recall that a proof system P is defined as

$$\varphi \in \text{TAUT} \text{ iff } \exists y P(y) = \varphi.$$

The set of propositional classical tautologies is *coNP*-complete. On the other hand, if the length of y is bounded by the length of φ, we get NP. □

Lengths of Proofs

Conjecture: NP $\neq$ coNP (which implies P $\neq$ NP)

Therefore, we expect that there is no polynomially bounded proof system, i.e., all proof systems have *intractable theorems*.

Program

Separate NP from coNP (and hence P from NP): show super-polynomial lower bounds to the length of proofs in all propositional proof systems.

Major achievements (classical proof systems)

There are exponential lower bounds to the lengths of proofs in several weak classical proof systems such as resolution, cutting planes, and bounded-depth Frege systems.
However, for strong systems, including Frege and extended Frege systems, no such lower bounds have been established.

Proof complexity of non-classical logics

By proving lower bounds to the lengths of proofs in non-classical proof systems, we separate complexity classes NP and PSPACE, which is supposedly easier than the NP vs. coNP problem. Thereof, we expect to have better results in the non-classical realm.
Confirmation to this intuition:

Theorem (Hrubeš (2007) and Jeřábek (2009))

There are exponential lower bounds for intuitionistic and modal Frege and extended Frege systems.

Unfortunately, and needless to say, the intuitionistic result cannot be used for classical logic, because the formulas have short proofs in classical Hilbert system.

Our contribution

Substructural logics are non-classical logics where some or all the usual structural rules are absent.

Theorem (weaker version)

Let L *be a substructural logic such that* $\mathsf{L} \subseteq \mathsf{IPC}$. *Then, there exists a sequence of* L*-tautologies that require exponentially long proofs in any Hilbert-style system for* L.

Our contribution

Substructural logics are non-classical logics where some or all the usual structural rules are absent.

Theorem (weaker version)

Let L *be a substructural logic such that* $\mathsf{L} \subseteq \mathsf{IPC}$. *Then, there exists a sequence of* L*-tautologies that require exponentially long proofs in any Hilbert-style system for* L.

Remark

If a sequence of formulas do not have short proofs in intuitionistic logic, then they will not have short proofs in substructural ones. Is the theorem above a trivial statement?

Our contribution

Substructural logics are non-classical logics where some or all the usual structural rules are absent.

Theorem (weaker version)

Let L *be a substructural logic such that* $\mathsf{L} \subseteq \mathsf{IPC}$. *Then, there exists a sequence of* L*-tautologies that require exponentially long proofs in any Hilbert-style system for* L.

Remark

If a sequence of formulas do not have short proofs in intuitionistic logic, then they will not have short proofs in substructural ones. Is the theorem above a trivial statement?

No. These intuitionistically valid formulas may not be provable in substructural logics. And that is the case here.

Superintuitionistic infinite branching logics

Consider the following superintuitionistic (si) logics:

$$\mathsf{KC} = \mathsf{IPC} + \neg p \vee \neg\neg p \qquad , \qquad \mathsf{BD_n} = \mathsf{IPC} + BD_n$$

where IPC is the intuitionistic logic and $BD_0 := \bot$ and $BD_{n+1} := p_n \vee (p_n \to BD_n)$.

Theorem (Jeřábek)

A si logic L *has infinite branching iff* $\mathsf{L} \subseteq \mathsf{BD_2}$ *or* $\mathsf{L} \subseteq \mathsf{KC} + \mathsf{BD_3}$.

Frege rules

Frege systems are the most natural calculi for propositional logic.

A **(Frege) rule** is an expression of the form

$$\frac{\varphi_1, \ldots, \varphi_k}{\varphi}$$

where $\varphi_1, \ldots, \varphi_k, \varphi$ are propositional formulas.

Let $\mathbf{P}$ be a finite set of rules. A $\mathbf{P}$-proof of φ from a set of assumptions X, denoted by $X \vdash_{\mathbf{P}} \varphi$, is $\varphi_1, \ldots, \varphi_m = \varphi$ such that each $\varphi_i \in X$, or is inferred from some φ_j, $j < i$, by a substitution instance of rule in $\mathbf{P}$. The formulas φ_i are called *lines* of the proof.

Frege systems

Now, we are ready to define Frege systems.

Definition

A finite set of rules, **P**, is called a *Frege system* for a logic L when

(1) **P** is strongly sound: if $\varphi_1, \ldots, \varphi_n \vdash_{\mathbf{P}} \varphi$, then $\varphi_1, \ldots, \varphi_n \vdash_{\mathsf{L}} \varphi$,

(2) **P** is strongly complete: if $\varphi_1, \ldots, \varphi_n \vdash_{\mathsf{L}} \varphi$, then $\varphi_1, \ldots, \varphi_n \vdash_{\mathbf{P}} \varphi$.

Example: Hilbert-style systems for classical and intuitionistic logics.

Substructural calculi

$$\varphi \Rightarrow \varphi \qquad \Rightarrow 1 \qquad 0 \Rightarrow$$

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, 1 \Rightarrow \Delta}\,(1w) \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow 0, \Delta}\,(0w)$$

$$\frac{\Gamma, \varphi \Rightarrow \Delta}{\Gamma, \varphi \wedge \psi \Rightarrow \Delta} \qquad \frac{\Gamma, \psi \Rightarrow \Delta}{\Gamma, \varphi \wedge \psi \Rightarrow \Delta} \qquad \frac{\Gamma \Rightarrow \varphi, \Delta \qquad \Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \wedge \psi, \Delta}$$

$$\frac{\Gamma, \varphi \Rightarrow \Delta \qquad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \varphi \vee \psi \Rightarrow \Delta} \qquad \frac{\Gamma \Rightarrow \varphi, \Delta}{\Gamma \Rightarrow \varphi \vee \psi, \Delta} \qquad \frac{\Gamma \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \vee \psi, \Delta}$$

$$\frac{\Gamma, \varphi, \psi \Rightarrow \Delta}{\Gamma, \varphi * \psi \Rightarrow \Delta} \qquad \frac{\Gamma \Rightarrow \varphi, \Delta \qquad \Sigma \Rightarrow \psi, \Lambda}{\Gamma, \Sigma \Rightarrow \varphi * \psi, \Delta, \Lambda}$$

$$\frac{\Gamma \Rightarrow \varphi, \Delta \qquad \Sigma, \psi \Rightarrow \Lambda}{\Gamma, \Sigma, \varphi \rightarrow \psi \Rightarrow \Delta, \Lambda} \qquad \frac{\Gamma, \varphi \Rightarrow \psi, \Delta}{\Gamma \Rightarrow \varphi \rightarrow \psi, \Delta}$$

$$\frac{\Gamma \Rightarrow \varphi, \Delta \qquad \Sigma, \varphi \Rightarrow \Lambda}{\Gamma, \Sigma \Rightarrow \Delta, \Lambda}\,(cut)$$

Substructural logics

The language of $\mathsf{FL_e}$ is $\{0, 1, \wedge, \vee, *, \rightarrow\}$. Uppercase Greek letters denote multisets of formulas.

- $\mathbf{FL_e}$: the single-conclusion version of the rules.
- $\mathbf{CFL_e}$: the multi-conclusion version of the rules.

Remark

Consider uppercase Greek letters to be *sequences* of formulas instead of multisets, i.e., the exchange rule is not present. Then, we introduce two implication-like connectives $\setminus$ and $/$, and include their respective rules. This system is called **FL**.

The logic FL is defined as the set of all formulas φ such that $\vdash_{\mathbf{FL}} \Rightarrow \varphi$.
Define $\vdash_{\mathsf{FL}}$ as: $\Gamma \vdash_{\mathsf{FL}} \varphi$ iff $\{\Rightarrow \gamma\}_{\gamma \in \Gamma} \vdash_{\mathbf{FL}} \Rightarrow \varphi$.
A *substructural logic* (over FL) is a set of formulas closed under both substitution and $\vdash_{\mathsf{FL}}$.

Structural rules

Weakening rules:

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, \varphi \Rightarrow \Delta}\,(i) \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \varphi, \Delta}\,(o)$$

Contraction rules:

$$\frac{\Gamma, \varphi, \varphi \Rightarrow \Delta}{\Gamma, \varphi \Rightarrow \Delta}\,(Lc) \qquad \frac{\Gamma \Rightarrow \varphi, \varphi, \Delta}{\Gamma \Rightarrow \varphi, \Delta}\,(Rc)$$

Structural rules

Weakening rules:

$$\frac{\Gamma \Rightarrow \Delta}{\Gamma, \varphi \Rightarrow \Delta}\,(i) \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \varphi, \Delta}\,(o)$$

Contraction rules:

$$\frac{\Gamma, \varphi, \varphi \Rightarrow \Delta}{\Gamma, \varphi \Rightarrow \Delta}\,(Lc) \qquad \frac{\Gamma \Rightarrow \varphi, \varphi, \Delta}{\Gamma \Rightarrow \varphi, \Delta}\,(Rc)$$

- $\mathbf{FL_{ei}} = \mathbf{FL_e} + (i)$, $\mathbf{FL_{eo}} = \mathbf{FL_e} + (o)$, $\mathbf{FL_{ew}} = \mathbf{FL_e} + (i) + (o)$,
- $\mathbf{CFL_{ei}}, \mathbf{CFL_{eo}}$ and $\mathbf{CFL_{ew}}$, similarly,
- $\mathbf{FL_{ec}} = \mathbf{FL_e} + (Lc)$,
- $\mathbf{CFL_{ec}} = \mathbf{CFL_e} + (Lc) + (Rc)$.

Basic substructural calculi

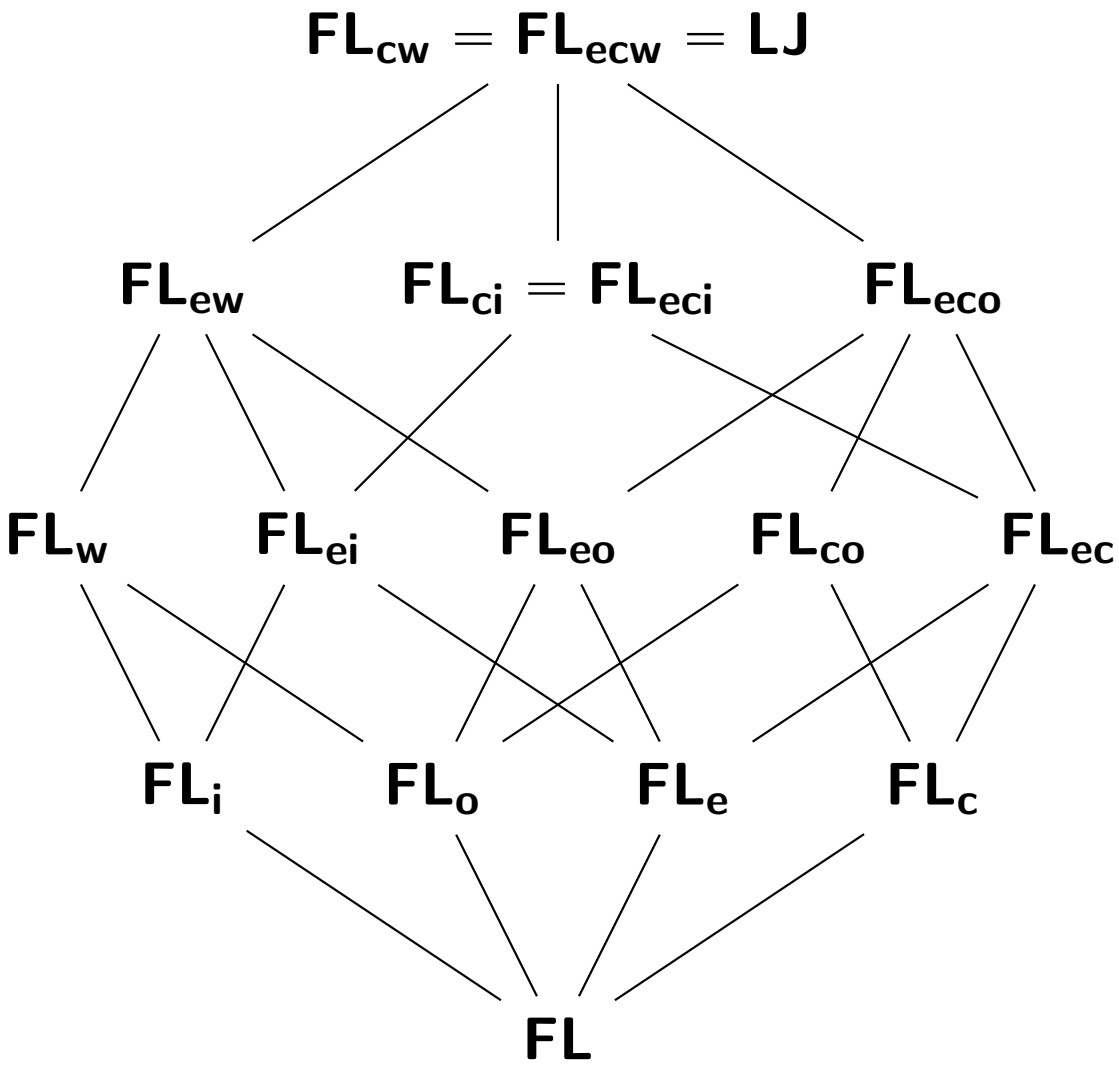

Table: Some sequent calculi with their definitions.

Sequent calculus	Definition
RL	$\mathbf{FL} + (0 \Leftrightarrow 1)$
CyFL	$\mathbf{FL} + (\varphi\backslash 0 \Leftrightarrow 0/\varphi)$
DFL	$\mathbf{FL} + (\varphi \wedge (\psi \vee \theta) \Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \theta))$
$\mathbf{P_nFL}$	$\mathbf{FL} + (\varphi^n \Leftrightarrow \varphi^{n+1})$
psBL	$\mathbf{FL_w} + \{(\varphi \wedge \psi \Leftrightarrow \varphi * (\varphi\backslash\psi)), (\varphi \wedge \psi \Leftrightarrow (\psi/\varphi) * \varphi)\}$
HA	$\mathbf{FL_w} + (\varphi \Leftrightarrow \varphi^2)$
DRL	$\mathbf{RL} + (\varphi \wedge (\psi \vee \theta) \Leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \theta))$
IRL	$\mathbf{RL} + (\varphi \Rightarrow 1)$
CRL	$\mathbf{RL} + (\varphi * \psi \Leftrightarrow \psi * \varphi)$
GBH	$\mathbf{RL} + \{(\varphi \wedge \psi \Leftrightarrow \varphi * (\varphi\backslash\psi)), (\varphi \wedge \psi \Leftrightarrow (\psi/\varphi) * \varphi)\}$
Br	$\mathbf{RL} + (\varphi \wedge \psi \Leftrightarrow \varphi * \psi)$

How to prove the lower bound

We have to provide a sequence of formulas provable in $\mathbf{FL_e}$, such that every proof of them are long.

- (Main task) providing a sequence of $\mathbf{FL_e}$-tautologies:
  Change the existing hard intuitionistic tautologies in a suitable way that they become provable in $\mathbf{FL_e}$, but remain hard.
- (Easier part) proving they are hard:
  Use the canonical translation of the language of $\mathbf{FL_e}$ to the language of IPC, i.e., sending $\{0, 1, *\}$ to $\{\bot, \top, \wedge\}$, respectively and the other connectives to themselves. This transformation takes polynomial time.

Hard intuitionistic tautologies

The following formulas, $\Theta_{n,k}$, are hard for IPC and they are negation-free and $\bot$-free. Small Roman letters denote atomic formulas and the formulas α_n^k and β_n^{k+1} are monotone, i.e., only consist of atoms, $\wedge$ and $\vee$.

Intuitionistic formulas:

$$\Theta_{n,k} := \bigwedge_{i,j}(p_{i,j} \vee q_{i,j}) \rightarrow$$

$$[(\bigwedge_{i,l}(s_{i,l} \vee s'_{i,l}) \rightarrow \alpha_n^k(\bar{p}, \bar{s}, \bar{s'})) \vee (\bigwedge_{i,l}(r_{i,l} \vee r'_{i,l}) \rightarrow \beta_n^{k+1}(\bar{q}, \bar{r}, \bar{r'}))]$$

Hard intuitionistic tautologies

The following formulas, $\Theta_{n,k}$, are hard for IPC and they are negation-free and $\bot$-free. Small Roman letters denote atomic formulas and the formulas α_n^k and β_n^{k+1} are monotone, i.e., only consist of atoms, $\wedge$ and $\vee$.

Intuitionistic formulas:

$$\Theta_{n,k} := \bigwedge_{i,j}(p_{i,j} \vee q_{i,j}) \rightarrow$$

$$[(\bigwedge_{i,l}(s_{i,l} \vee s'_{i,l}) \rightarrow \alpha_n^k(\bar{p}, \bar{s}, \bar{s'})) \vee (\bigwedge_{i,l}(r_{i,l} \vee r'_{i,l}) \rightarrow \beta_n^{k+1}(\bar{q}, \bar{r}, \bar{r'}))]$$

Theorem (Hrubeš '07, Jeřábek '09)

The formulas $\Theta_{n,k}$ are IPC*-tautologies and require* IPC*-Frege proofs with $2^{n^{\Omega(1)}}$ lines, for $k = \lfloor\sqrt{n}\rfloor$.*

Hard FL_e-tautologies

Define the following formulas

$$\Theta^*_{n,k} := [\underset{i,j}{\divideontimes}((p_{i,j} \wedge 1) \vee (q_{i,j} \wedge 1))] \quad \rightarrow$$

$$[(\underset{i,l}{\divideontimes}((s_{i,l} \wedge 1) \vee (s'_{i,l} \wedge 1)) \rightarrow \alpha^k_n) \ \vee (\underset{i,l}{\divideontimes}((r_{i,l} \wedge 1) \vee (r'_{i,l} \wedge 1)) \rightarrow \beta^{k+1}_n)]$$

Hard FL_e-tautologies

Define the following formulas

$$\Theta^*_{n,k} := [\underset{i,j}{\divideontimes}((p_{i,j} \wedge 1) \vee (q_{i,j} \wedge 1))] \rightarrow$$

$$[(\underset{i,l}{\divideontimes}((s_{i,l} \wedge 1) \vee (s'_{i,l} \wedge 1)) \rightarrow \alpha^k_n) \vee (\underset{i,l}{\divideontimes}((r_{i,l} \wedge 1) \vee (r'_{i,l} \wedge 1)) \rightarrow \beta^{k+1}_n)]$$

Theorem

The formulas $\Theta^*_{n,k}$ are FL_e-tautologies. Moreover, for any substructural logic L and any superintuitionistic logic of infinite branching M such that $\mathsf{FL}_e \subseteq \mathsf{L} \subseteq \mathsf{M}$, the formulas $\Theta^*_{n,k}$ require L-Frege proofs with $2^{n^{\Omega(1)}}$ lines, for $k = \lfloor \sqrt{n} \rfloor$.

Applications

Corollary

Let $S \subseteq \{e, c, i, o\}$, and L *be* FL_S*, or any of the logics of the sequent calculi in Table 1. Then the length of every proof of Θ_n^* in any (extended) Frege system for* L *is exponential in n.*

Applications

Corollary

Let $S \subseteq \{e, c, i, o\}$, and L *be* FL_S*, or any of the logics of the sequent calculi in Table 1. Then the length of every proof of Θ_n^* in any (extended) Frege system for* L *is exponential in n.*

What happens in the case of the classical versions of the above substructural logics? They are not included in IPC and hence our method does not work. However, for their cut-free versions we have the following theorem.

Theorem

The length of every proof of Θ_n^* in the sequent calculi $\mathbf{CFL}_{\mathbf{e}}^{-}, \mathbf{CFL}_{\mathbf{ei}}^{-}, \mathbf{CFL}_{\mathbf{eo}}^{-}$, and $\mathbf{CFL}_{\mathbf{ew}}^{-}$ is exponential in n, where the "$-$" means without the cut rule.

Thank you for your attention.